

Session # 1

*Information Security:
What is it and why is
it needed?*



Content Notes

Presentation Notes

Welcome participants to the Information Security is Good Business seminar.

Introduce yourself: name, qualifications, background (briefly).

Point out locations of facilities:

- Telephones
- Restrooms
- Emergency Exits
- Refreshments

Session # 1

*Information Security:
What is it and why is
it needed?*



Presenters

Alicia Clay, Ph.D.

*Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology*

James Schifalacqua, CISSP

*Chief Technologist
Information Security
SI International, Inc.*

Session # 1

*Information Security:
What is it and why is
it needed?*



The NIST Mission

To develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

Page 3

Content Notes

The National Institute of Standards and Technology (NIST) develops and promotes measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

Presentation Notes

Refer to examples of real life applications: MRI, gasoline pumps, etc.

Session # 1

Information Security:
What is it and why is
it needed?



Getting Acquainted

Introductions:

- Name
- Type of business
- Distance traveled



Page 4

Content Notes

Presentation Notes

Conduct a warm up activity:

Introductions/Interviews

Time: 5-10 minutes

Materials: none

Goal: accelerate comfort level, promote interaction among participants, get general information

Set-up: works with any set-up. If participants are seated at tables, have them introduce themselves to the table group. If there are no tables, ask participants to introduce themselves to **3** other people in their area.

Procedure:

Ask participants to:

1. Introduce themselves to each person (or to the table group)
2. Give name, type of business, general location of business, and distance traveled to the meeting.
3. Allow 5 minutes.

Session # 1

Information Security:
What is it and why is
it needed?



Getting Acquainted

- Who represents an unusual type of business?
- What type of business has the greatest representation?
- Who traveled the greatest distance?



Page 5

Mouse click
for each
question

Content Notes

Presentation Notes

Report out:

Ask for a show of hands for each of these questions:

Ask: "Who met someone representing a unique type of business?"

Call on a few people and repeat the type of business for the whole group.

Ask: "From the conversations you have had, what type of business do you think has the greatest representation today?" (medical office, lawyers, retail merchant, etc.)

Call on someone for an answer and then ask for a show of hands to see how many participants have the type of business named.

Repeat the question 1 - 3 more times to get an idea of which, if any, types of companies/organizations have the largest representation.

Ask: "Who met someone they believe came the greatest distance for today's meeting?"

Call on all those who raise their hands and ask them to introduce the person who traveled a distance.

Session # 1

*Information Security:
What is it and why is
it needed?*



Goal

Promote:

- Awareness of the importance and need for IT security
- Understanding of IT security vulnerabilities and corrective measures



Page 6

Content Notes

Presentation Notes

Transition by repeating your welcome to all participants, from whatever type of business or organization, and from whatever distance they may have come.

Encourage attendees to introduce themselves to others during breaks and to exchange business cards.

Explain the goal of today's meeting.

Point out that, by the end of the day, attendees will understand both IS problems and appropriate solutions for their situations.

Session # 1

*Information Security:
What is it and why is
it needed?*



You Will Learn:

- How your data is vulnerable
- What you can lose through an IS breach
- Practical steps to protect your business
- How to use IS vendors and consultants
- How to evaluate tools and techniques based on your needs

Page 7

Presentation Notes

Review the day's objectives.
(These are taken from the NIST
web site.)

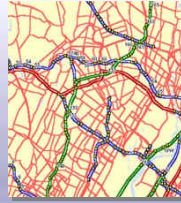
Session # 1

*Information Security:
What is it and why is
it needed?*



Resource Materials

- Agenda/Roadmap
- PowerPoint Notes
- Evaluations
- CD



Page 8

Session # 1

*Information Security:
What is it and why is
it needed?*



Agenda

Information Security is Good Business:
Tools and Techniques

Morning Sessions

Open/Welcome

1. Information Security...What is it and why is it needed?
2. Information Security...Why Invest?
3. Information Security...Defining Your Needs
4. Common Information Security Practices

Lunch

Afternoon Sessions

4. Common Information Security Practices (*Continued*)
5. Information Security...The Mechanisms and Technologies

Page 9

Session # 1

*Information Security:
What is it and why is
it needed?*



Content Notes

Presentation Notes

Expand (briefly) on your IS and instructional background.

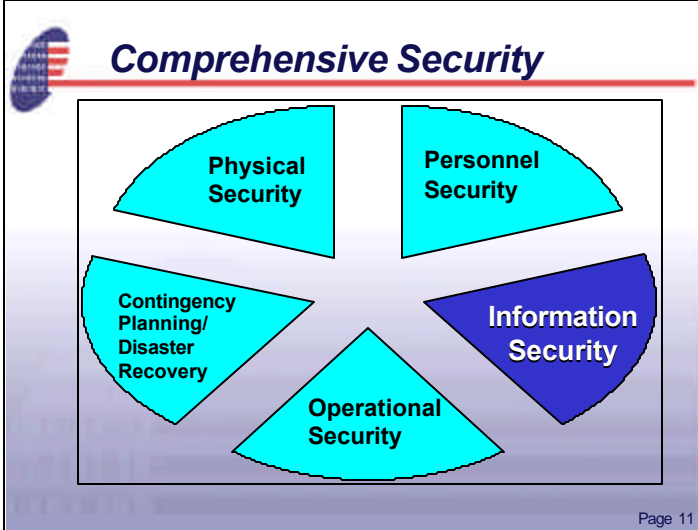
Point out the focus of this first presentation is to

- Define Information Security
- Demonstrate the necessity of IS to businesses and organizations
- Give examples of the most common types of threats to information security

Emphasize that the goal of the presentations is to empower the attendees to protect their information.

Session # 1

Information Security:
What is it and why is
it needed?



Content Notes

Before we look at details of Information Security it is important to point out that InfoSec is only part of a comprehensive security effort

Physical Security

- Protection of Life and Property
- An Essential Element of Information Access Control

Personnel Security

- Background Checks
- Behavioral Monitoring

Contingency Planning and Disaster Recovery

- Includes planning for not being able to use your computer
- Includes planning for when your critical IT person leaves/resigns.
- Well understood, but not always implemented and tested

Operational Security

- Protection of your private business intentions
- Dealing with the Media, External Organizations

As well as Information Security.

Lacking any one piece (physical, personnel, etc.) diminishes the effectiveness of the other pieces of the security puzzle.

Presentation Notes

Explain that all these aspects of security are interrelated and interdependent.

Session # 1

*Information Security:
What is it and why is
it needed?*



What is Information Security?

Tools and techniques that protect an organization's:



Page 12

Content Notes

Information Security: Those attributes of a system that provide Information and system assets protection

Our purpose today is to talk about those tools and techniques – from restricting employee access to your critical data to installing protection against the most recent virus attack.

Presentation Notes

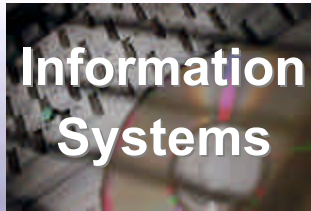
Session # 1

*Information Security:
What is it and why is
it needed?*



What is Information Security?

Tools and techniques that protect an organization's:



Page 13

Content Notes

Information Security: Those attributes of a system that provide Information and system assets protection

Our purpose today is to talk about those tools and techniques – from restricting employee access to your critical data to installing protection against the most recent virus attack.

Presentation Notes

Give a few examples of information systems

Session # 1

Information Security:
What is it and why is
it needed?



Characteristics of InfoSec

- Confidentiality
- Integrity
- Availability



Page 14

Content Notes

Information Security: Those attributes of a system that provide information and system assets protection

- **Confidentiality** (protection from unauthorized view or possession)
- **Integrity** (protection from unauthorized modification or removal)
- **Availability** (having information and processes available when needed)

Confidentiality, Integrity, Availability is often shortened to “**CIA**”

Sometimes “Accountability” (knowing what, who, when, and how information is accessed) is added to the list of “CIA”, but accountability is more of a management issue rather than a security property.

Bottom line for you is keeping your

- **Business**
- **Employees**
- **Customers**

safe, secure, and available.

Information Security is all about maintaining proper control over your information

Presentation Notes

Explain each attribute.

Give brief examples for each. Point out that they will need to prioritize these attributes when it they develop a security policy and do security risk assessment.

Explain how accountability is more of a management issue – how it has more to do with control than with protection.

Give example.

Session # 1

*Information Security:
What is it and why is
it needed?*



Today's Threats

Computer Security Institute/FBI Survey*:

- **85% reported security breaches.**
- 70% from outside organization
- 30% from inside organization
- **91% reported employee Internet abuse**



*2000

Page 15

Content Notes

CSI/FBI 2001 Computer Crime and Industry Survey:

- 85% of respondents detected security breaches within the past 12 months
- Of those attacked, 70% originated from the Internet (outside), and 30% originated from inside

Presentation Notes

Introduce the slide by pointing out that, nationally, breaches in IS are already having an impact on businesses.

Session # 1

*Information Security:
What is it and why is
it needed?*



Today's Threats (Continued)

Computer Security Institute/FBI Survey:

➤ Attacks results

- 64% in financial losses (\$377,828,700)
- 34% could quantify loss
- 90% in vandalism



Page 16

Content Notes

CSI/FBI 2001 Computer Crime and Industry Survey:

- 64% resulted in financial losses; 34% could quantify those
 - Total reported loss: \$377,828,700
- 91% detected employee abuse of Internet
- 90% of websites that were attacked resulted in vandalism

Presentation Notes

Ask: These statistics are pretty impressive. How many of you know personally of a business that suffers/has suffered from any of these problems?

Ask for a show of hands as a lead in to the next slide.

Session # 1

Information Security:
What is it and why is
it needed?



Not Just Big Guys

32%
Small Businesses



Page 17

Content Notes

32% of respondents from small business

Presentation Notes

Explain that about 32% of those who replied were small businesses. This means that some of the types of businesses represented in today's meeting may have been among them.

Session # 1

Information Security:
What is it and why is
it needed?



Web Defacement and Break-In

Large and small businesses

- A “Big Bank” to a small electronics store
- Over 6,000 in 2000 – www.attrition.org



Page 18

Content Notes

Many sites/victims were businesses, large and small

“Big Bank”

Small electronics store in Pennsylvania

Over 6,000 sites in year 2000 - www.attrition.org

Does not always require breaking into the server

Web software often allows users to “come right in”

Presentation Notes

Tell attendees that some registrants indicated that the web was part of their business...

Session # 1

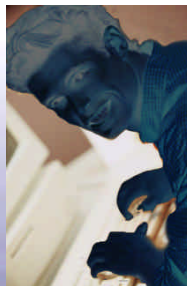
Information Security:
What is it and why is
it needed?



Who are the bad guys?

Amateurs Through Experts:

- Experimenters and Vandals
- Hacktivists
- Cybercriminals
- Information warriors



Page 19

Content Notes

Hacker spectrum runs from the amateur, through the expert, to the deadly:

Experimenters and Vandals: Use tools from the Internet to take down your website and computers to impress their peers and leave their mark

Hacktivists: Have a personal or political agenda to destroy, embarrass, and blackmail your company

Cybercriminals: Steal your customers' credit cards and account information

Information Warriors: State-supported professionals who want to disrupt the Internet and all computers connected to it.

Presentation Notes

Explain how an amateur hacker can have an impact.

Emphasize that it is lack of awareness that makes users susceptible.

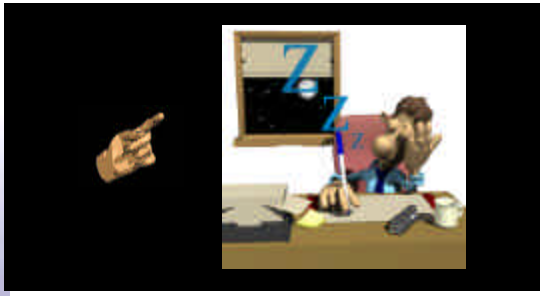
Discuss briefly why experimenters might want to do this.

Explain why a state might support such professionals.

Mouse click for
each bullet



Their common target?



You

Content Notes

Presentation Notes

Session # 1
*Information Security:
What is it and why is
it needed?*



Content Notes

This is a site where you can enter the name and address of a computer and have the site itself try to break in to it.

URL: <http://bluemoon.virtual-power.net/start.html>

Presentation Notes

Session # 1

Information Security:
What is it and why is
it needed?



Why do People Do This?

- Bragging rights/global attention
- Political activism (hactivism)
- Grudge or intentional harm



Page 27

Content Notes

Why do people do this?

Bragging rights, global attention

Political activism (hactivism)

Grudge or intention to harm a company

Presentation Notes

Ask which motivation most often affects small businesses.

Call on participants for answers.

Explain how answers apply to small businesses.

Session # 1

*Information Security:
What is it and why is
it needed?*



Potential Consequences

- Embarrassment
- Repair costs
- Misinformation or worse
- Loss of eBusiness



Page 28

Content Notes

Potential Consequences
Credibility
Down time
Misled customers
Loss of business

Presentation Notes

Give examples:

Lost credibility: your website could post insulting or derogatory statements.

Misled customers: the customer service phone numbers on your website might be changed.

Session # 1

*Information Security:
What is it and why is
it needed?*



Three Common Attacks Today

- Theft of data and resources
- Denial-of-service attacks
- Malicious codes and viruses



Page 29

Content Notes

Presentation Notes

Explain that you will discuss each type of attack in more detail...

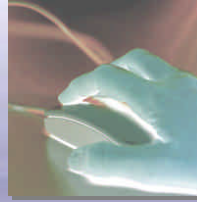
Session # 1

*Information Security:
What is it and why is
it needed?*



Theft of Data and Resources

- **Stealing your computer files**
- **Accessing your computer accounts**
- **Stealing your laptops and computers**
- **Intercepting your e-mail**



Page 30

Content Notes

Theft of Data and Resources

- Getting in to your computer and printing, copying, etc. your private files
- Someone else using your computer account
- Stealing Laptops and Computers
- Intercepting your e-mail and Internet exchanges

Presentation Notes

Explain how this could happen.

Explain how this could happen.

Session # 1

Information Security:
What is it and why is
it needed?



Maxus Extortion Case

- Stole 300,000 credit card numbers
- Attempted a \$100,000 extortion
- Offered 25,000 credit cards numbers on website



Page 31

Content Notes

Maxus, the 18-year-old Russian hacker who:

- Stole 300,000 credit card numbers from a music CD ordering company
- Stole 300,000 credit card numbers
- Then tried to extort \$100,000 from the company to not reveal these credit card numbers
- When the company resisted, he offered 25,000 credit cards numbers on Web site

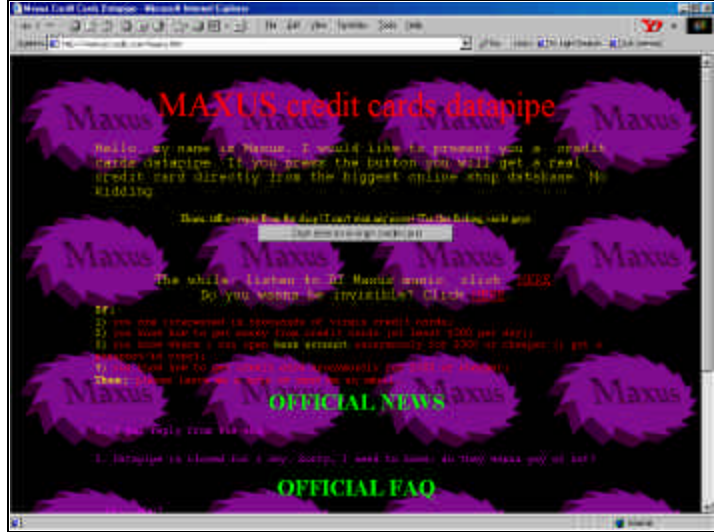
We're not completely sure how he got them, but a combination of some poor website configuration and some Internet attack tools were the likely factors

Although Maxus was never apprehended, two Russian hackers who tried something similar were lured into the U.S. by offer of employment, and then arrested by the FBI

Presentation Notes

Note: Could substitute Infragard presentation for Maxus slides.

Session # 1
Information Security:
What is it and why is it needed?



Content Notes

The actual Maxus website from which he conducted business...

Presentation Notes

Session # 1

Information Security:
What is it and why is
it needed?



Denial-of-Service Attacks

Attacking your computer or website

- Locks up equipment
- Crashes your systems

Results

- Stops/slows work workflow
- Prevents e-mail communications
- Shuts down eCommerce

Page 33

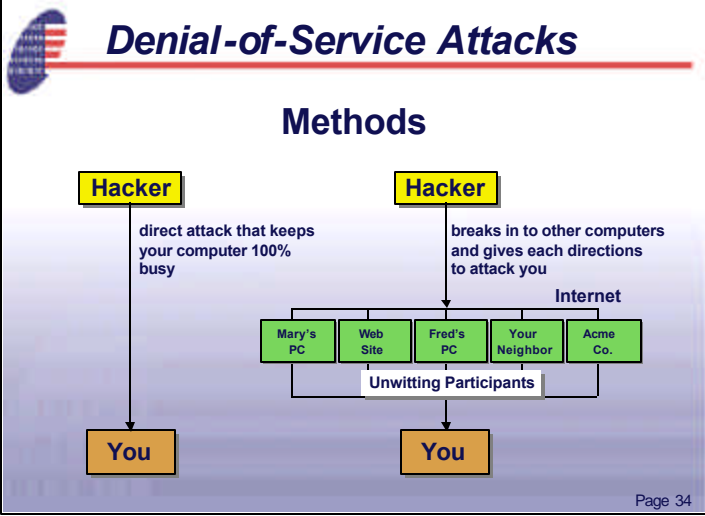
Content Notes

Denial-of-service attacks

- Locking up your computer or website so that no one else can use it
- Maybe even crashing it completely
- Keeping you from doing any work, receiving any mail, getting any online orders. (Examples of denial of service are: Web sit-ins, e-mail bombs.)

Presentation Notes

Explain that an “e-mail bomb” means that someone sends you thousands of duplicate emails, overloading your computer system



Content Notes

Presentation Notes

Session # 1

Information Security:
What is it and why is
it needed?



Malicious Code

- Sends itself over Internet
- Sends your files over Internet
- Deletes your data
- Locks up your computer or system
- Hides in program or documents
- Copies itself

Page 35

Content Notes

Malicious Code:

Any software on your computer that you don't know about, which is (maybe at this very moment):

- Sending itself or your files out over the Internet
- Deleting your data
- Locking up your computer

Virus:

Hides in a program or document

- Copies itself from system to system, file to file, disk to disk

More than 70,000 viruses exist

- E-mail is the most common means of infection

Malicious code can also exist as worms and Trojan horse.

Presentation Notes

Explain that when system administrators were asked, 85% of them rated viruses, malicious code as their most time consuming problem. They also said: "Biggest problem with security is the lack of employee training and end-user awareness."

Session # 1

Information Security:
What is it and why is
it needed?



Malicious Code

◀ Trojan horse



◀ Virus



◀ Worm



Page 36

Content Notes

Trojan Horses Programs which masquerade as something useful or amusing, but do something unexpected, such as:

- Stealing passwords, credit card numbers, files, keystrokes
- Launching DoS attacks or worms/viruses
- Sabotage, especially by insiders (time bombs)
- Usually sent inside a game, such as "Whack a Mole"
- BackOrifice, NetBus, etc. (User can then remotely monitor and control a computer)

Worm: Program that spreads itself from system to system across the network

Virus:

W97.Class

- Infects Word documents using Word macro features
- Triggers on the 14th of the month from June through December
- Displays a message that is "personally insulting" to the user ("I think [user name] is a big stupid jerk")

Melissa

- Also infects Word documents
- Sends e-mail to first n addresses of Outlook Address Book
- Attaches an infected Word document to the message

Presentation Notes

Mouse click for each bullet.

Session # 1

Information Security:
What is it and why is
it needed?



The Hoax as the Perfect Virus

E-mails with false warnings about a virus

Classic symptoms of a hoax virus:

- Message source
- Warnings of doom and destruction
- Technical jargon
- Directions to pass it on



Page 37

Content Notes

Shows up in an email as a false warning about a virus

- Causes panic, systems to be shut down
- Causes email systems to be overwhelmed by forwarded messages
- Relies on well-meaning, but misinformed users to propagate the “virus”

Classic symptoms of a hoax virus:

- Message source is “from a friend of a friend”
 - Authoritative sources cited such as IBM, FAA, ...
- Warnings of Doom and Destruction
- Lots of Technical Jargon
- You are implored to “Pass it on!” to everyone you know
- No verifiable reference to an anti-virus vendor or security alert

Examples:

- Good Times, Pictures From a Friend, Deeyenda, Join The Crew, Win a Holiday, ...
- They all resulted in a lot of wasted time, unfounded fear, and “junk” email clogging up people’s mailboxes

Presentation Notes

Explain that a hoax is similar to a vicious chain letter.

Session # 1

Information Security:
What is it and why is
it needed?



Even the People You Know

- Malicious actions
- Unintentional damage
- Non-business use of computers



Page 38

Content Notes

Inappropriate Actions By Insiders

Malicious actions by employees/insiders

- Accessing salaries, personnel files, or private customer data
- Sending unauthorized communications
- Making unauthorized business decisions
 - Snooping around the computer files, seeing what they can get (salaries, personnel files, private data)
 - Breaking in to your computer, pretending to be you

Non-business related use of computers

- Web Browsing by employees to inappropriate, non-business related sites (pornography, hate sites, ...)
- Sending harassing e-mails
- Hacking to outside systems
- Potentially high employer liability when employees perform these actions

Presentation Notes

Introduce slide material:

“Who is responsible for this type of damage?”

Mention that company policies on employee use of web and email vary. Explain that every company should have a policy and that the topic will be explored in a later presentation.

Session # 1

*Information Security:
What is it and why is
it needed?*



What Should You Do About It?

Your organization's information:

- Is as vital as equipment, staff, and buildings
- Requires the same protection
- Has become more vulnerable with the use of Computers and Networks

Take control of your information security with:

- Analysis
- People
- Procedures
- Technology

Page 39

Content Notes

Your Information Assets are as vital to your business as your physical assets, your people, and your product

- Business requires the proper collection, processing, and dissemination of information (picture of this process for a business, rather than words)
- Information Security is all about maintaining proper control over your information
- Information Security has direct analogies to protecting your buildings, your offices, your physical records, and your people from harm and misuse

But your computers and networks may have become much more accessible (and vulnerable) than all of the above

If you care about your customers, you care about security. Identity theft is now an important concern. Do not ask private questions in public.

Presentation Notes

Emphasize that “although you may think of information security as technology, such as firewalls or virus detection, successful information security really involves much more, and we are going to look at that bigger picture today.”

NOTE: Ask participants to take a few minutes to fill out the evaluation form for this presentation, which is at the end of the presentation handout. Put the filled out evaluation form on the table at the back of the room.